**Practitioner's Docket No. NAI1P718/01.261.01** *PATENT*

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Swati Deshmukh et al.

Application No.: 10/067,319 Group No.: 2441
Filed: 02/07/2002 Examiner: Nguyen, Quang N.
For: SYSTEM AND METHOD FOR REAL-TIME TRIGGERED EVENT UPLOAD

**Mail Stop Appeal Briefs – Patents**
**Commissioner for Patents**
**P.O. Box 1450**
**Alexandria, VA 22313-1450**

## TRANSMITTAL OF APPEAL BRIEF
## (PATENT APPLICATION--37 C.F.R. § 41.37)

1. This brief is in furtherance of the Notice of Appeal filed 09/29/2006, a substitute for the Substitute Appeal Brief filed 02/05/2007, and in response to the Notification of Non-Compliant Appeal Brief mailed on 10/31/2008.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

| | |
|---|---|
| other than a small entity | $540.00 |
| **Appeal Brief fee due** | **$540.00** |

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

| | |
|---|---|
| Appeal brief fee | $0.00 (previously paid 11/29/2006) |
| Extension fee (if any) | $0.00 |
| **TOTAL FEE DUE** | **$0.00** |

6. FEE PAYMENT

Applicant believes that no fees are due in connection with the filing of this paper because the Appeal Brief fee was paid with a previous submission. However, the Commissioner is authorized to charge any additional fees that may be due (e.g. for any reason including, but not limited to, fee changes, etc.) to Deposit Account No. 50-1351 (Order No. NAI1P718).

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P718).

Date: December 1, 2008

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

/KEVINZILKA/
Signature of Practitioner
Kevin J. Zilka
Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

**PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re application of: | |
| Deshmukh et al. | Group Art Unit: 2441 |
| Application No. 10/067,319 | Examiner: Nguyen, Quang N. |
| Filed: 02/07/2002 | Atty. Docket No.<br>NAI1P718/01.261.01 |
| For: SYSTEM AND METHOD FOR REAL-TIME TRIGGERED EVENT UPLOAD | Date: 12/01/2008 |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences**

**SUBSTITUTE APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal filed 09/29/2006, a substitute for the Substitute Appeal Brief filed 02/05/2007, and in response to the Notification of Non-Compliant Appeal Brief mailed on 10/31/2008 (see attached). While appellant disagrees with the Examiner as to whether the alleged deficiencies exist in the original Appeal Brief, a Substitute Appeal Brief with appropriate edits is nevertheless submitted to expedite prosecution.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES
III STATUS OF CLAIMS
IV STATUS OF AMENDMENTS
V SUMMARY OF CLAIMED SUBJECT MATTER
VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
VII ARGUMENT
VIII CLAIMS APPENDIX
IX EVIDENCE APPENDIX
X RELATED PROCEEDING APPENDIX

The final page of this brief bears the practitioner's signature.

## I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

## II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

## III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

### A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 16-17, 32-33, and 48-81 .

### B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration: None
2. Claims pending: 1, 16-17, 32-33, and 48-81
3. Claims allowed: None
4. Claims rejected: 1, 16-17, 32-33, and 48-81
5. Claims cancelled: 2-15, 18-31, and 34-47

### C. CLAIMS ON APPEAL

The claims on appeal are: 1, 16-17, 32-33, and 48-81

See additional status information in the Appendix of Claims.

## IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

## V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 1, and 4 et al., a method of reporting malware events comprises the steps of detecting a plurality of malware events (e.g. see item 406 of Figure 4, etc.) each with one of a plurality of levels using a malware scanner (e.g. see item 116 of Figure 1, etc.). The plurality of malware events comprises completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware. Further, the method comprises the step of determining a level of a detected malware event (e.g. see item 410 of Figure 4, etc.). Additionally, the method comprises the step of comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels (e.g. see item 412 of Figure 4, etc.). In addition, the method comprises the step of transmitting a notification of the detected malware event (e.g. see item 414 of Figure 4, etc.) over a network (e.g. see item 104 of Figure 1, etc.), based on the comparison of the level of the detected malware event to the event trigger threshold. See, for example, page 4, lines 2-17 et al.

Furthermore, the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 4, line 16 – page 5, line 2 et al.

Additionally, the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 5, lines 3-9 et al.

In addition, the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold. Further still, the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network. See, for example, page 4, lines 2-4; page 5, lines 12-17; and page 18, lines 1-5 et al.

With respect to a summary of Claim 17, as shown in Figures 1, 2, and 4 et al., a system for reporting malware events comprises a processor (e.g. see item 202 of Figure 2, etc.) operable to execute computer program instructions. Further, the system comprises a memory (e.g. see item 208 of Figure 2, etc.) operable to store computer program instructions executable by the processor. In addition, the system comprises computer program instructions stored in the memory that are executable to perform the steps of detecting a plurality of malware events (e.g. see item 406 of Figure 4, etc.) each with one of a plurality of levels using a malware scanner (e.g. see item 116 of Figure 1, etc.). The plurality of malware events comprises completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware. In addition, the computer program instructions are stored in the memory and are executable to perform the steps of determining a level of a detected malware event (e.g. see item 410 of Figure 4, etc.), comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels (e.g. see item 412 of Figure 4, etc.), and transmitting a notification of the detected malware event (e.g. see item 414 of Figure 4, etc.) over a network (e.g. see item 104 of Figure 1, etc.), based on the comparison of the level of the detected malware event to the event trigger threshold. See, for example, page 4, lines 2-17; page 9, lines 12-15; and page 10, lines 15-17 et al.

Furthermore, the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 4, line 16 – page 5, line 2 et al.

In addition, the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 5, lines 3-9 et al.

Additionally, the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold. Further still, the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network. See, for example, page 4, lines 2-4; page 5, lines 12-17; and page 18, lines 1-5 et al.

With respect to a summary of Claim 33, as shown in Figures 1, 2, and 4 et al., a computer program product for reporting malware events comprises a computer readable storage medium (e.g. see item 208 of Figure 2, etc.). Further, the computer program product comprises computer program instructions, recorded on the computer readable storage medium, executable by a processor (e.g. see item 202 of Figure 2, etc.), for performing the steps of detecting a plurality of malware events (e.g. see item 406 of Figure 4, etc.) each with one of a plurality of levels using a malware scanner (e.g. see item 116 of Figure 1, etc.). The plurality of malware events comprises completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware. In addition, the computer program instructions perform the steps determining a level of a detected malware event (e.g. see item 410 of Figure 4, etc.), comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels (e.g. see item 412 of Figure 4, etc.), and transmitting a notification of the detected malware event (e.g. see item 414 of Figure 4, etc.) over a network (e.g. see item 104 of Figure 1., etc.), based on the comparison of the level of the detected malware event to the event trigger threshold. See, for example, page 4, lines 2-17; page 9, lines 12-15; and page 10, lines 15-17 et al.

Furthermore, the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 4, line 16 – page 5, line 2 et al.

In addition, the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; and critical malware events that need immediate operator attention and could lead to loss of data if not corrected. See, for example, page 5, lines 3-9 et al.

Additionally, the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold. Further still, the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network. See, for example, page 4, lines 2-4; page 5, lines 12-17; and page 18, lines 1-5 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

## VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has rejected Claims 1, 16-17, 32-33, and 48-81 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (U.S. Patent Publication 2003/0131256), in view of Hansen et al. (U.S. Patent No 6,493,755).

## VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has rejected Claims 1, 16-17, 32-33, and 48-81 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (U.S. Patent Publication 2003/0131256), in view of Hansen et al. (U.S. Patent No 6,493,755).

*Group #1: Claims 1*, 16-17, 32-33, and 48-81

Appellant respectfully asserts that Ackroyd discloses a managing computer within a computer network that logs messages received from individual computers within that computer network indicating detection of malware. The managing computer detects patterns of malware detection across the network as a whole as triggers associated predetermined anti-malware actions. These may include forcing specific computers to update their malware definition data, forcing particular computers to change their security settings and isolating individual portions of the computer network. However, Ackroyd does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant.

Additionally, appellant respectfully asserts that Hansen discloses a network management application that provides notification of events on network devices using prepopulated notification rules. The notification rule is prepopulated by the network management application using conditions that represent the present state of the device being monitored. An associated notification action is executed when an event on a network device satisfies the conditions of the prepopulated notification rule. However, Hansen does not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant.

Thus, even if Ackroyd and Hansen were combined as suggested by the Examiner, the resulting combination of Ackroyd and Hansen still would not disclose or suggest an event trigger threshold that is configurable to control the amount of notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network, as claimed by appellant in Claims 1, 17, and 33.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest <u>all</u> of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

## VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A method of reporting malware events comprising the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

2.-15. (Cancelled)

16. (Previously Presented) The method of claim 1, wherein the method further comprises the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

17. (Previously Presented) A system for reporting malware events comprising:

a processor operable to execute computer program instructions;

a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

18.-31. (Cancelled)

32. (Previously Presented) The system of claim 17, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

33. (Previously Presented) A computer program product for reporting malware events, comprising:

a computer readable storage medium;

computer program instructions, recorded on the computer readable storage medium, executable by a processor, for performing the steps of

detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;

determining a level of a detected malware event;

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and

transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;

wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

34.-47. (Cancelled)

48. (Previously Presented) The computer program product of claim 33, further comprising the step of:

transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold.

49. (Previously Presented) The method of claim 1, wherein the event trigger threshold is set at a management server in a malware management program.

50. (Previously Presented) The method of claim 49, wherein the event trigger threshold is set by setting policies in the malware management program.

51. (Previously Presented) The method of claim 1, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

52. (Previously Presented) The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

53. (Previously Presented) The method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

54. (Previously Presented) The method of claim 1, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

55. (Previously Presented) The method of claim 54, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

56. (Previously Presented) The method of claim 54, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

57. (Previously Presented) The method of claim 54, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

58. (Previously Presented) The method of claim 54, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

59. (Previously Presented) The method of claim 54, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

60. (Previously Presented) The system of claim 17, wherein the event trigger threshold is set at a management server in a malware management program.

61. (Previously Presented) The system of claim 60, wherein the event trigger threshold is set by setting policies in the malware management program.

62. (Previously Presented) The system of claim 17, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

63. (Previously Presented) The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

64. (Previously Presented) The system of claim 17, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

65. (Previously Presented) The system of claim 17, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:

(1) the informational malware events requiring no operator intervention;

(2) the warning malware events that indicate a process failure;

(3) the minor malware events that require attention, but are not events that could lead to loss of data;

(4) the major malware events that need operator attention; and

(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

66. (Previously Presented) The system of claim 65, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

67. (Previously Presented) The system of claim 65, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

68. (Previously Presented) The system of claim 65, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

69. (Previously Presented) The system of claim 65, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

70. (Previously Presented) The system of claim 65, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

71. (Previously Presented) The computer program product of claim 33, wherein the event trigger threshold is set at a management server in a malware management program.

72. (Previously Presented) The computer program product of claim 71, wherein the event trigger threshold is set by setting policies in the malware management program.

73. (Previously Presented) The computer program product of claim 33, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems.

74. (Previously Presented) The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission.

75. (Previously Presented) The computer program product of claim 33, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received.

76. (Previously Presented) The computer program product of claim 33, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from a least critical to a most critical with progressively greater levels, as follows:
(1) the informational malware events requiring no operator intervention;
(2) the warning malware events that indicate a process failure;
(3) the minor malware events that require attention, but are not events that could lead to loss of data;
(4) the major malware events that need operator attention; and
(5) the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

77. (Previously Presented) The computer program product of claim 76, wherein the completion of the malware scan corresponds to one of the informational malware events requiring no operator intervention.

78. (Previously Presented) The computer program product of claim 76, wherein the process failure relating to the malware scanning corresponds to one of the warning malware events that indicate a process failure.

79. (Previously Presented) The computer program product of claim 76, wherein the missing log file corresponds to one of the minor malware events that require attention, but are not events that could lead to loss of data.

80. (Previously Presented) The computer program product of claim 76, wherein the detection of the malware corresponds to one of the major malware events that need operator attention.

81. (Previously Presented) The computer program product of claim 76, wherein the failure of the response to the malware corresponds to one of the critical malware events that need immediate operator attention and could lead to loss of data if not corrected.

## IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

## X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P718).

Respectfully submitted,

By: /KEVINZILKA/ Date: December 1, 2008
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/067,319 | 02/07/2002 | Swati Deshmukh | 19903.0016 | 7037 |

23517 7590 10/31/2008

BINGHAM MCCUTCHEN LLP
2020 K Street, N.W.
Intellectual Property Department
WASHINGTON, DC 20006

| EXAMINER |  |
|---|---|
|  |  |
| ART UNIT | PAPER NUMBER |
|  |  |

DATE MAILED: 10/31/2008

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|---|---|---|---|
| ***Notification of Non-Compliant Appeal Brief (37 CFR 41.37)*** | **Application No.**<br>10/067,319 | **Applicant(s)**<br>DESHMUKH ET AL. | |
| | **Examiner**<br>QUANG NGUYEN | **Art Unit**<br>2441 | |

***--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

The Appeal Brief filed on _05 February 2007_ is defective for failure to comply with one or more provisions of 37 CFR 41.37.

To avoid dismissal of the appeal, applicant must file anamended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. □ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. □ The brief does not contain a statement of the status of all claims, (e.g., rejected, allowed, withdrawn, objected to, canceled), or does not identify the appealed claims (37 CFR 41.37(c)(1)(iii)).

3. □ At least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment (37 CFR 41.37(c)(1)(iv)).

4. ☒ (a) The brief does not contain a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings, if any, by reference characters; and/or (b) the brief fails to: (1) identify, for each independent claim involved in the appeal and for each dependent claim argued separately, every means plus function and step plus function under 35 U.S.C. 112, sixth paragraph, and/or (2) set forth the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification by page and line number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(v)).

5. □ The brief does not contain a concise statement of each ground of rejection presented for review (37 CFR 41.37(c)(1)(vi))

6. □ The brief does not present an argument under a separate heading for each ground of rejection on appeal (37 CFR 41.37(c)(1)(vii)).

7. □ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(viii)).

8. □ The brief does not contain copies of the evidence submitted under 37 CFR 1.130, 1.131, or 1.132 or of any other evidence entered by the examiner **and relied upon by appellant in the appeal**, along with a statement setting forth where in the record that evidence was entered by the examiner, as an appendix thereto (37 CFR 41.37(c)(1)(ix)).

9. □ The brief does not contain copies of the decisions rendered by a court or the Board in the proceeding identified in the Related Appeals and Interferences section of the brief as an appendix thereto (37 CFR 41.37(c)(1)(x)).

10. ☒ Other (including any explanation in support of the above items):

_The claimed invention does not separately refer to the independent claims 1,17 and 33, which shall refer to the specification by page and line number and to the drawings, if any. An entire brief is not required just the defective section should be submitted ._

SHARMALLA COATES
SUPERVISORY PATENT APPEAL CENTER SPECIALIST